CLAIMS

We claim:

1. A method for verifying port mapping integrity in a network, comprising:

accessing port binding information in a port authorization file in said network;

querying a port mapper for a mapped port assignment;

comparing said port assignment to said port binding information; and

initiating a response to said comparing.

2. The method described in Claim 1 wherein said network comprises a utility data center.

3. The method described in Claim 1 wherein said port assignment comprises static port binding data.

4. The method described in Claim 1 wherein said port authorization file comprises fixed port assignments.

5. The method described in Claim 1 wherein said port authorization file is generated upon network initialization.

6. The method described in Claim 1 wherein said response comprises an alarm.

7. The method described in Claim 1 wherein said response comprises a system lockdown.

8. In a network comprising a plurality of network port connections, a network port map verification tool, comprising:

a port assignment file comprising a port authorization in said network; and

a port assignment file verifier, wherein said verifier is enabled to verify a port assignment against said port authorization.

9. The port map verification tool described in Claim 9, wherein said network comprises a utility data center.

10. The port map verification tool described in Claim 9, wherein said port map verification tool is further enabled to initiate a response to a port assignment anomaly.

11. The port map verification tool described in Claim 11, wherein said response is an alarm.

12. The port map verification tool described in Claim 11, wherein said response is a system lockdown.

13. The port map verification tool described in Claim 9, wherein said port map verification tool is enabled to verify a digital signature related to said port authorization.

14. The port map verification tool described in Claim 9, wherein said tool is enabled to operate in a remote procedure call environment.

15. A system for protecting network security, comprising:

a network server;

a network client communicatively coupled with said server via a port;

a plurality of provisionable services enabled to communicate with said server via a plurality of ports; and

a port map verification tool enabled to compare a port assignment to a port authorization in said network.

16. The system for protecting network security described in Claim 17 wherein said network comprises a utility data center.

17. The system for protecting network security described in Claim 17, wherein said port map verification tool is enabled to initiate a response to a port assignment anomaly.

18. The system for protecting network security described in Claim 17, wherein said response can be an alarm.

19. The system for protecting network security described in Claim 17, wherein said response can be a system lockdown.

20. The system for protecting network security described in Claim 17, wherein said tool is enabled to operate in a remote procedure call environment.